

Generalized Greatest Common Divisors for the Orbits under Rational Functions

Keping Huang *

Abstract

Assume Vojta's Conjecture (Conjecture 2.1). Suppose $a, b, \alpha, \beta \in \mathbb{Z}$, and $f(x), g(x) \in \mathbb{Z}[x]$ are polynomials of degree $d \geq 2$. Assume that the sequence $(f^{\circ n}(a), g^{\circ n}(b))_n$ is generic and α, β are not exceptional for f, g respectively, we prove that for each given $\varepsilon > 0$, there exists a constant $C = C(\varepsilon, a, b, \alpha, \beta, f, g) > 0$, such that for all $n \geq 1$, we have

$$\gcd(f^{\circ n}(a) - \alpha, g^{\circ n}(b) - \beta) \leq C \cdot \exp(\varepsilon \cdot d^n).$$

We prove an estimate for rational functions and for a more general gcd and then obtain the above inequality as a consequence.

1 Introduction

In [5], Bugeaud, Corvaja, and Zannier proved the following theorem.

Theorem 1.1. *Let a, b be multiplicatively independent integers ≥ 2 , and let $\varepsilon > 0$. Then, provided n is sufficiently large, we have*

$$\gcd(a^n - 1, b^n - 1) < \exp(\varepsilon n).$$

The authors of that paper obtained the result by contradiction. They began by constructing finitely many vectors in terms of n, a , and b . Then they showed that if the bound is not satisfied, then the vectors must lie in a lower-dimensional linear subspace by the Schmidt Subspace Theorem. Using this result they are able to derive algebraic relations on powers of a and b , which guarantee that a, b are multiplicatively dependent.

One may ask whether a similar inequality holds for iterations of polynomials, as iterations are dynamical analogues of power maps. It seems that current tools are not powerful enough to tackle this problem. An important progress was made in [15], where Silverman observed that one can interpret the greatest common divisor as a height function on some blow-up of the projective plane. Furthermore, assuming Vojta's Conjecture (cf. [20]), Silverman also gave in [18] reasonably strong upper bounds for the greatest common divisor of the values of some polynomial functions, in terms of the absolute values of the initial points. See also [14] for an application of Silverman's

*keping.huang@rochester.edu, Department of Mathematics, University of Rochester

method to gcd bounds for analytic functions. Many other authors have worked out various generalization and variations of this problem, both over number fields and function fields (see [1], [6], [7], [8] and [17] for example).

In this paper, we apply Silverman's method in the situation of iterations. In fact, we will prove a Silverman-type estimate for a fixed smaller iteration, and derive some results on gcd's. However, there are some technical difficulties. First, in order to have the required operands of the greatest common divisor, one needs to blow up a proper Zariski closed subset in general (as opposed to subvarieties in [18]), depending on the prescribed constant ϵ . Second, in the case of the rational functions the numerators of iterates might not be iterates of any polynomial, so we need a more detailed analysis. We also need to control the degree of ramification, for this we also need the reasonable assumption that α, β are not exceptional.

Let X be an algebraic variety defined over $\overline{\mathbb{Q}}$. We say that a sequence $(x_n)_n \subseteq X$ is *generic* in X if for any proper Zariski closed subset $Y \subsetneq X$, there exists an $N \in \mathbb{N}$ such that for all $n \geq N$, $x_n \notin Y$. A point $x_0 \in \overline{\mathbb{Q}}$ is said to be *exceptional* for a rational function $\phi \in \overline{\mathbb{Q}}(x)$ if the backward orbit $\cup_{n=0}^{\infty} \phi^{-n}(\{x_0\})$ is finite.

A main result of this paper is the following theorem.

Theorem A. *Assume Vojta's Conjecture (Conjecture 2.1). Suppose $a, b, \alpha, \beta \in \mathbb{Z}$, and that $f(x), g(x) \in \mathbb{Z}[x]$ are polynomials of degrees $d \geq 2$. Assume that α, β are not exceptional for f, g respectively. Assume that the sequence $(f^{on}(a), g^{on}(b))_n$ is generic in $\overline{\mathbb{Q}}^2$. Then for each given $\varepsilon > 0$, there exists a constant $C = C(\varepsilon, a, b, \alpha, \beta, f, g) > 0$, such that for all $n \geq 1$, we have*

$$\gcd(f^{on}(a) - \alpha, g^{on}(b) - \beta) \leq C \cdot \exp(\varepsilon \cdot d^n).$$

Remark. *The result is trivial when $d_1 \neq d_2$, and is proved in [6] for the case $d_1 = d_2 = 1$. We use the convention that $\gcd(0, 0) = 0$. But this involves only finitely many n , since the sequence $(f^{on}(a), g^{on}(b))_n$ is generic, and hence so is $(f^{on}(a) - \alpha, g^{on}(b) - \beta)_n$.*

In [21] Xie proved the Dynamical Mordell-Lang Conjecture for polynomial endomorphisms of the affine plane. Therefore the genericity of the sequence $(f^{on}(a), g^{on}(b))_n$ is equivalent to the Zariski density of $(f^{on}(a), g^{on}(b))_n$. On the other hand, Medvedev and Scanlon gave in [12] characterizations of periodic curves under split polynomial endomorphisms of $\mathbb{P}^1(\overline{\mathbb{Q}}) \times \mathbb{P}^1(\overline{\mathbb{Q}})$. The equation of the curve should meet certain commutativity conditions, which are unlikely to hold in general. Therefore the genericity condition of the sequence $(f^{on}(a), g^{on}(b))_n$ is a mild condition.

Actually we will prove a generalization of Theorem A and obtain Theorem A as a consequence. In [18] Silverman defined a more general gcd height which is log of gcd in the case of rational integers. In the same paper he proved most results in this more general framework. See section 2 for the precise definitions and statements.

The plan of this paper is as follows. Section 2 contains a table of notations, a statement of Vojta's Conjecture, some results concerning the gcd height, and statements of other main theorems of this paper. We prove our main theorem concerning the gcd height in Section 3. In Section 4, we first cite a genericity criterion for the case when $f = g$ are non-special polynomials, replacing the genericity condition. We also cite a

theorem of Corvaja and Zannier for the case of power maps. At the end of Section 4 we give several examples to explain why the genericity condition in Theorem A is necessary; our policy is to include only results which are easy to state and hopefully clarify things greatly.

2 Preliminaries

We use the following notations throughout this paper.

K	a number field.
$M(K), n_v$	the set of places of K ; the product formula has power n_v for the place v .
f, g	rational functions defined over K .
d	the degree of f and g .
h	a Weil height on K .
\hat{h}_f	the canonical height with respect to f .
f^{on}	the n -th iterate of f .

We will use the following version of Vojta's Conjecture. For a thorough discussion of Vojta's Conjecture, see the monograph [20].

Conjecture 2.1 (Vojta). *Let K be a number field, and let X be a nonsingular variety defined over K . Suppose A is an ample normal-crossing divisor on X and K_X is the canonical divisor of X , both defined over K . Let h_A and h_{K_X} be the corresponding height functions respectively. For each fixed $\varepsilon > 0$, there is a Zariski closed proper subset V of X and a constant C such that*

$$h_{K_X}(x) \leq \varepsilon \cdot h_A(x) + C$$

for all $x \in X(K) \setminus V(K)$.

We briefly recall Silverman's idea. For all $v \in M(\mathbb{Q})$ and $a \in \mathbb{Z}$, let $v^+(a) = \max(-\log |a|_v, 0) \in [0, +\infty]$. Silverman began his discussion in [15] by writing the greatest common divisor as

$$\log \gcd(a, b) = \sum_{v \in M(\mathbb{Q})} \min(v^+(a), v^+(b)) \quad (2.1)$$

for $a, b \in \mathbb{Z}$. Then he extends this function for $a, b \in \mathbb{Q}$ by the same formula. Using the ideas from [15], Silverman observed that the above quantity can be interpreted as a height function with respect to some subschemes, and furthermore as a height function on some blown-up surface. In fact, for algebraic variety X , Silverman defined in [15] a height function $h_{X,Y}$ with respect to any closed subschemes Y . These generalized functions also satisfy certain functorial property. More generally, the following definition is a slight generalization of that given by Silverman in [18].

Definition 2.2 ([18]). *Let K be a number field and let X/K be a smooth variety. Let $Y/K \subsetneq X/K$ be a subscheme of codimension $r \geq 2$. Let $\pi : \tilde{X} \rightarrow X$ be the*

blowup of X along Y , and let $\tilde{Y} = \pi^{-1}(Y)$ be the exceptional divisor of the blowup. For $x \in (X - Y)(K)$, we let $\tilde{x} = \pi^{-1}(x) \in \tilde{X}$. The generalized (logarithmic) greatest common divisor of the point $x \in (X - Y)(K)$ with respect to Y is the quantity

$$h_{\text{gcd}}(x; Y) = h_{X,Y}(x) = h_{\tilde{X},\tilde{Y}}(\tilde{x}).$$

By abuse of notation, for a number fields K and for $a, b \in K$ we also define the generalized gcd as

$$h_{\text{gcd}}(a, b) = \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M(K)} n_v \min(v^+(a), v^+(b)). \quad (2.2)$$

We also define

$$h_{\text{gcd},\text{fin}}(a, b) = \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M(K), \text{fin}} n_v \min(v^+(a), v^+(b)). \quad (2.3)$$

Then clearly $h_{\text{gcd},\text{fin}} \leq h_{\text{gcd}}$.

As a consequence of the Weil height machine, the relationship between these two h_{gcd} is shown as below. See [15] and [18] for some interesting cases over \mathbb{Z} where the contribution from the places at infinity is zero or bounded. Suppose K is a number field. Let $X = \mathbb{P}^1(\overline{\mathbb{Q}}) \times \mathbb{P}^1(\overline{\mathbb{Q}})$ and let $f(X_1) \in K[X_1], g(X_2) \in K[X_2]$ be polynomials. Then over $\overline{\mathbb{Q}}$ the vanishing set $Z(f)$ and $Z(g)$ define two divisors D_1 and D_2 on X . Set $Y = D_1 \cap D_2$. Then for all points $x = (x_1, x_2) \in \mathbb{P}^1(\overline{\mathbb{Q}}) \times \mathbb{P}^1(\overline{\mathbb{Q}})$ with $x_1, x_2 \in K$, such that $f(x_1) \neq 0$ and $g(x_2) \neq 0$, we have

$$\begin{aligned} h_{\text{gcd}}(f(x_1), g(x_2)) &= h_{\mathbb{P}^1(\overline{\mathbb{Q}}) \times \mathbb{P}^1(\overline{\mathbb{Q}}), (0,0)}(f(x_1), g(x_2)) \\ &= h_{\mathbb{P}^1(\overline{\mathbb{Q}}) \times \mathbb{P}^1(\overline{\mathbb{Q}}), (f,g)^*(0,0)}(x_1, x_2) \\ &= h_{\text{gcd}}(x; Y) + O(1), \end{aligned}$$

where the second equality follows from Theorem 2.1(h) of [15].

Our goal is to prove the following theorem.

Theorem 2.3. *Assume Vojta's Conjecture (Conjecture 2.1). Let K be a number field. Suppose $a, b, \alpha, \beta \in K$. Let $f, g \in K(x)$ with degree $\deg f = \deg g = d \geq 2$. Assume that the sequence $(f^{on}(a) - \alpha, g^{on}(b) - \beta)_n \subseteq \mathbb{P}^1(\overline{\mathbb{Q}}) \times \mathbb{P}^1(\overline{\mathbb{Q}})$ is generic, and α and β are not exceptional for f and g respectively. Then for each given $\varepsilon > 0$, there exists a constant $C = C(\varepsilon, a, b, \alpha, \beta, f, g)$ such that for all $n \geq 1$, we have*

$$h_{\text{gcd}}(f^{on}(a) - \alpha, g^{on}(b) - \beta) \leq \varepsilon \cdot d^n + C.$$

We can also conclude the periodicity of an irreducible component of the Zariski closure $\overline{(f^n(a), g^n(b))_n}$ under (f, g) in the cases when the Dynamical Mordell-Lang Conjecture is proved. See Section 4.

Thanks to the powerful theorems proved in [2], [12], and [13], we can give some concrete conditions for $(f^n(a), g^n(b))_n$ being generic in the case when $f = g$ are so-called non-special polynomials (See Section 4).

Theorem 2.4. *Assume Vojta's Conjecture (Conjecture 2.1). Let K be a number field and $f \in K[x]$ be a polynomial of degree $d \geq 2$. Assume that f is not conjugate (by a rational automorphism defined over $\overline{\mathbb{Q}}$) to a power map or a Chebyshev map. Suppose $a, b, \alpha, \beta \in K$ and α, β are not exceptional for f . Assume that there is no polynomial $h \in \overline{\mathbb{Q}}[x]$ such that $h \circ f^{\circ k} = f^{\circ k} \circ h$ for some $k \in \mathbb{N}_{>0}$ and $h(f^{\circ m}(a)) = b$ or $h(f^{\circ m}(b)) = a$ for some $m \in \mathbb{N}$, then for any $\varepsilon > 0$, there exists a $C = C(\varepsilon, a, b, \alpha, \beta, f, g) > 0$ such that for all $n \geq 1$, we have*

$$h_{\text{gcd}}(f^{\circ n}(a) - \alpha, f^{\circ n}(b) - \beta) \leq \varepsilon \cdot d^n + C.$$

3 The Proof of Theorem 2.3

We first prove the following modification of Theorem 2 of Silverman ([18]). Recall that a one-variable polynomial over a field K is called *reduced* if it does not have repeated roots in \overline{K} .

Theorem 3.1. *Let K be a number field. Suppose $f \in K[X_1]$ and $g \in K[X_2]$ are reduced polynomials in one variable, Then the scheme-theoretical intersection*

$$Y = Z(f) \cap Z(g) \subseteq \mathbb{P}^1(\overline{\mathbb{Q}}) \times \mathbb{P}^1(\overline{\mathbb{Q}})$$

is a reduced cycle of codimension 2.

Assume that Vojta's conjecture is true (for $\mathbb{P}^1(\overline{\mathbb{Q}}) \times \mathbb{P}^1(\overline{\mathbb{Q}})$ blown up along Y). Fix $\varepsilon > 0$. Then there is a algebraic subset $V \subsetneq \mathbb{P}^1(\overline{\mathbb{Q}}) \times \mathbb{P}^1(\overline{\mathbb{Q}})$, depending on f, g and ε , so that every $P = (x_1, x_2) \in \mathbb{P}^1(K) \times \mathbb{P}^1(K)$ satisfies either

1. $P \in V$, or
2. $h_{\text{gcd}}(f(x_1), g(x_2)) \leq (3 + \varepsilon)(h(x_1) + h(x_2)) + O(1)$.

Proof of Theorem 3.1. We follow the proof in [18]. Suppose $Z(f) = \{\alpha_1, \dots, \alpha_m\}$, $Z(g) = \{\beta_1, \dots, \beta_n\}$. Then $Y = \cup_{1 \leq i \leq m, 1 \leq j \leq n} \{(\alpha_i, \beta_j)\}$, each with multiplicity one. Also elements in $Z(f)$ and $Z(g)$ meet transversally, hence Y is a reduced cycle of codimension 2. To simplify notations write $Y = \{Q_1, \dots, Q_s\}$. Let $\pi : \tilde{X} \rightarrow X$ be the blowup of $X = \mathbb{P}^1(\overline{\mathbb{Q}}) \times \mathbb{P}^1(\overline{\mathbb{Q}})$ along Y and let \tilde{Y} be the preimage of Y . Then \tilde{X} is a smooth variety.

It follows that

$$K_{\tilde{X}} = \pi^* K_X + \tilde{Y}_1 + \dots + \tilde{Y}_s$$

where each \tilde{Y}_i is the preimage of Q_i . We can choose $-K_X$ to be a normal crossing divisor. By Definition 2 of [18], we still have $h_{\text{gcd}}(P; Y) = h_{\tilde{X}, \tilde{Y}}(\tilde{P})$.

To apply Vojta's Conjecture, let $A \in \text{Div}(X)$ be a divisor of type $(1, 1)$ and consider the \mathbb{Q} -divisor

$$\tilde{A} := \pi^* A - \frac{1}{N} (\tilde{Y}_1 + \dots + \tilde{Y}_s) \in \text{Div}(\tilde{X}) \otimes \mathbb{Q}.$$

We claim that \tilde{A} is ample when $N > s$. For this we begin with the following lemma.

Lemma 3.2 ([11], Chapter 1, Exercise 7.5(a)). *An irreducible curve Y of degree $d > 1$ in \mathbb{P}^2 cannot have a point of multiplicity $\geq d$.* \square

Now let $C \subseteq \mathbb{P}^1(\overline{\mathbb{Q}}) \times \mathbb{P}^1(\overline{\mathbb{Q}})$ be an irreducible curve of type (a, b) . Let \tilde{C} be its strict transform. By change of coordinate and restricting to the affine part, we know that C cannot have a point of multiplicity $\geq \deg(C)$. Now let $p_i : C \rightarrow \mathbb{P}^1$ be the projection to the i -th coordinate. Then $\deg p_1 = a, \deg p_2 = b$. It follows that $\deg(C) \leq a + b$. By the projection formula, we have

$$(\pi^* A. \tilde{C}) = (A. \pi_* \tilde{C}) = (A. C) = a + b.$$

Then

$$\begin{aligned} (\tilde{A}. \tilde{C}) &= (\pi^* A. \tilde{C}) - \frac{1}{N} \left((\tilde{Y}_1. \tilde{C}) + \cdots + (\tilde{Y}_s. \tilde{C}) \right) \\ &= a + b - \frac{1}{N} (\text{mult}_{Q_1}(C) + \cdots + \text{mult}_{Q_s}(C)) \\ &\geq a + b - \frac{1}{N} \cdot s \cdot (a + b) \\ &> 0 \end{aligned}$$

as $N > s$. Since Y_i 's are preimages of distinct Q_i 's, so $(\tilde{Y}_i, \tilde{Y}_j) = -\delta_{ij}$ and

$$\begin{aligned} (\tilde{A}. \tilde{Y}_i) &= (\pi^* A. \tilde{Y}_i) - \frac{1}{N} \left((\tilde{Y}_1. \tilde{Y}_i) + \cdots + (\tilde{Y}_s. \tilde{Y}_i) \right) \\ &= 0 - \frac{1}{N} (-\delta_{1i} - \cdots - \delta_{si}) \\ &= \frac{1}{N}. \end{aligned}$$

Finally by the previous equality

$$\begin{aligned} (\tilde{A}. \tilde{A}) &= (\tilde{A}. \pi^* A) - \frac{1}{N} \left((\tilde{A}. \tilde{Y}_1) + \cdots + (\tilde{A}. \tilde{Y}_s) \right) \\ &> \left(\pi_* \tilde{A}. A \right) - \frac{1}{N} \cdot \frac{s}{N} \\ &= (A. A) - \frac{s}{N^2} \\ &\geq 1 + 1 - \frac{s}{N^2} \\ &> 0 \end{aligned}$$

as $N > s$. But

$$\text{Pic}(\tilde{X}) = \pi^* \text{Pic}(X) \bigoplus_{i=1}^s \tilde{Y}_i,$$

and every effective curve C in \tilde{X} is linearly equivalent to a nonnegative combination of \tilde{Y}_i 's and the strict transform of effective curves in X , so \tilde{A} is ample by the Nakai-Moishezon criterion (see Chapter 5, Theorem 1.10 of [11]). Now assuming Vojta's Conjecture we have

$$h_{\tilde{X}, K_{\tilde{X}}}(\tilde{P}) \leq \varepsilon \cdot h_{\tilde{X}, \tilde{A}}(\tilde{P}) + C_\varepsilon$$

for all $P \in X(K) \setminus V(K)$. Also $K_{\tilde{X}} = \pi^* K_X + \tilde{Y}$ and $\tilde{A} = \pi^* A - 1/N \cdot \tilde{Y}$, so

$$\begin{aligned} h_{\tilde{X}, \pi^* K_X}(\tilde{P}) + h_{\tilde{X}, \tilde{Y}}(\tilde{P}) &\leq \varepsilon \cdot h_{\tilde{X}, \pi^* A}(\tilde{P}) - \frac{1}{N} \cdot h_{\tilde{X}, \tilde{Y}}(\tilde{P}) + C_\varepsilon, \\ h_{X, K_X}(P) + \left(1 + \frac{1}{N}\right) h_{\tilde{X}, \tilde{Y}}(P) &\leq \varepsilon \cdot h_{X, A}(P) + C'_\varepsilon, \\ \left(1 + \frac{1}{N}\right) h_{\text{gcd}}(P; Y) &\leq \varepsilon \cdot h_{X, A}(P) + h_{X, -K_X}(P) + C'_\varepsilon, \\ h_{\text{gcd}}(P; Y) &\leq \varepsilon \cdot h_{X, A}(P) + h_{X, -K_X}(P) + C''_\varepsilon. \end{aligned}$$

Since K_X is linearly equivalent to $-2A$, and let $P = (x_1, x_2)$. Then

$$\begin{aligned} h_{X, -K_X}(P) &= 2 \cdot (h(x_1) + h(x_2)) + O(1), \\ h_{X, A}(P) &= h(x_1) + h(x_2), \\ h_{\text{gcd}}(P; Y) &= h_{\text{gcd}}(f(x_1), g(x_2)). \end{aligned}$$

Now Theorem 3.1 is verified. □

Proof of Theorem 2.3. We begin with the following

Lemma 3.3. *Let $\sigma, \tau \in K(x)$ be Möbius transformations. Set $f_\sigma = \sigma f \sigma^{-1}$, $g_\tau = \tau g \tau^{-1}$. Then there exists a constant $C > 0$, depending on $\alpha, \beta, f, g, \sigma, \tau$, such that for all $a, b \in K$, and for all $n \in \mathbb{N}$, we have*

$$|h_{\text{gcd}, \text{fin}}(f_\sigma^{\circ n}(\sigma a) - \sigma \alpha, g_\tau^{\circ n}(\tau b) - \tau \beta) - h_{\text{gcd}, \text{fin}}(f^{\circ n}(a) - \alpha, g^{\circ n}(b) - \beta)| \leq C.$$

Proof. It suffices to show that for any fixed $\alpha \in K$, and for any fixed Möbius transformation σ , there exists a finite set $S \subset M(K)_{\text{fin}}$ and a constant $C' > 0$, such that for all $x \in K$ and $v \in S$, we have $|v^+(\sigma x - \sigma \alpha) - v^+(x - \alpha)| \leq C'$, and for all $x \in K$ and $v \in M(K)_{\text{fin}} \setminus S$, we have $v^+(\sigma x - \sigma \alpha) = v^+(x - \alpha)$.

Since each Möbius transformation defined over K is a composition of translations, dilations and inverses defined over K , it suffices to prove the result for the case when σ is one of the above three types of maps. The result is trivial for translations and dilations.

If $\sigma(x) = 1/x$, write $x = x_1/x_2, \alpha = \alpha_1/\alpha_2$, $x_1, x_2, \alpha_1, \alpha_2 \in \mathcal{O}_K$. Since the class number of K is finite, there exists $\gamma \in \mathcal{O}_K$ such that for fixed $\alpha \in \mathcal{O}_K$ and for all $x \in \mathcal{O}_K$ we can always choose $x_1, x_2, \alpha_1, \alpha_2$ such that the ideals $\text{gcd}(x_1, x_2) \mid \gamma$, $\text{gcd}(\alpha_1, \alpha_2) \mid \gamma$. Now

$$|x - \alpha|_v = \left| \frac{\alpha_2 x_1 - \alpha_1 x_2}{\alpha_2 x_2} \right|_v, \quad |\sigma x - \sigma \alpha|_v = \left| \frac{\alpha_2 x_1 - \alpha_1 x_2}{\alpha_1 x_1} \right|_v.$$

But the ideal

$$\begin{aligned} \text{gcd}(\alpha_2 x_1 - \alpha_1 x_2, \alpha_2 x_2) \mid \text{gcd}(\alpha_2^2 x_1 - \alpha_1 \alpha_2 x_2, \alpha_1 \alpha_2 x_2) &= \text{gcd}(\alpha_2^2 x_1, \alpha_1 \alpha_2 x_2) \\ &\mid \text{gcd}(\alpha_1 \alpha_2^2 x_1, \alpha_1 \alpha_2^2 x_2) \mid \alpha_1 \alpha_2^2 \gamma, \end{aligned}$$

so

$$v^+(\alpha_2 x_1 - \alpha_1 x_2) - v(\alpha_1 \alpha_2^2 \gamma) \leq v^+(x - \alpha) \leq v^+(\alpha_2 x_1 - \alpha_1 x_2).$$

Similarly

$$v^+(\alpha_2 x_1 - \alpha_1 x_2) - v(\alpha_1^2 \alpha_2 \gamma) \leq v^+(\sigma x - \sigma \alpha) \leq v^+(\alpha_2 x_1 - \alpha_1 x_2).$$

Therefore

$$|v^+(\sigma x - \sigma \alpha) - v^+(x - \alpha)| \leq \max(v(\alpha_1 \alpha_2^2), v(\alpha_1^2 \alpha_2 \gamma)) \leq v(\alpha_1^2 \alpha_2^2 \gamma).$$

Hence we may choose $S = \{v \in M(K)_{\text{fin}} \mid v(\alpha_1) \neq 0, v(\alpha_2) \neq 0 \text{ or } v(\gamma) \neq 0\}$. \square

Therefore for $h_{\text{gcd}, \text{fin}}$ we may assume that $\alpha = \beta = 0$. For any fixed integer D , write in the lowest terms $f^{\circ D} = F_1/F_2$ and $g^{\circ D} = G_1/G_2$ where F_1, F_2, G_1, G_2 are polynomials with coefficients in \mathcal{O}_K . For the same reason we may also assume that all D -th preimages of 0 under f and g are not ∞ .

Write

$$\begin{aligned} F_1(x) &= a_0 + \cdots + a_N x^N, \\ F_2(x) &= b_0 + \cdots + b_M x^M, \\ G_1(x) &= a'_0 + \cdots + a'_{N'} x^{N'}, \\ G_2(x) &= b'_0 + \cdots + b'_{M'} x^{M'} \end{aligned}$$

with all coefficients in \mathcal{O}_K . Then $N \geq M$. Let

$$S := \{\text{non-archimedean place } v \mid v(a_N) \neq 0, v(b_M) \neq 0, v(a'_{N'}) \neq 0, \text{ or } v(b'_{M'}) \neq 0\}.$$

Then S is finite. For all non-archimedean place $v \notin S$ and for any $x_0 \in K$, if $v(x_0) \geq 0$, then $v(F_2(x_0)) \geq 0$ and hence $v^+(f^{\circ D}(x_0)) \leq v^+(F_1(x_0))$. If $v(x_0) < 0$, then

$$v^+(f^{\circ D}(x_0)) = v^+\left(\frac{a_N x_0^N}{b_M x_0^M}\right) = v^+(x_0^{N-M}) = 0 \leq v^+(F_1(x_0)).$$

In either case we have

$$v^+(f^{\circ D}(x_0)) \leq v^+(F_1(x_0)).$$

Similarly for any $v \notin S$ and for any $y_0 \in K$,

$$v^+(g^{\circ D}(y_0)) \leq v^+(G_1(y_0)).$$

Therefore the sum of the finite parts of h_{gcd} outside S satisfy

$$\begin{aligned} h_{\text{gcd}, S}(f^{\circ D}(a'), g^{\circ D}(b')) &:= \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M(K)_{\text{fin}} \setminus S} n_v \min(v^+(f^{\circ D}(a')), v^+(g^{\circ D}(b'))) \\ &\leq \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M(K)_{\text{fin}} \setminus S} n_v \min(v^+(F_1(a')), v^+(G_1(b'))) \\ &\leq h_{\text{gcd}, S}(F_1(a'), G_1(b')). \end{aligned} \tag{3.1}$$

Let $F_1^{\text{red}}(x) = \text{rad}(F_1)(x)$, and let $G_1^{\text{red}}(y) = \text{rad}(G_1)(y)$, where for a one-variable polynomial P , $\text{rad}(P)$ is the product of all monic irreducible polynomials dividing

P . As the sequence $(f^{\circ(n-D)}(a), g^{\circ(n-D)}(b))_n$ is generic in $\mathbb{P}^1(\overline{\mathbb{Q}}) \times \mathbb{P}^1(\overline{\mathbb{Q}})$, there exists $N'' = N''(\varepsilon, f, g, a, b, \alpha, \beta)$, such that for all $n \geq N''$ we have

$$(f^{\circ(n-D)}(a), g^{\circ(n-D)}(b)) \notin V(K)$$

where V is as in Theorem 3.1. Apply Theorem 3.1 to the point $(f^{\circ(n-D)}(a), g^{\circ(n-D)}(b))$ and the functions F_1^{red} and G_1^{red} , with $\varepsilon = 1$. Let $u = f^{\circ(n-D)}(a), v = g^{\circ(n-D)}(b)$. Then

$$h_{\text{gcd}}(F_1^{\text{red}}(u), G_1^{\text{red}}(v)) \leq 4(h(u) + h(v)) + O(1). \quad (3.2)$$

Set

$$M' = \max_{f^{\circ D}(x)=\alpha, g^{\circ D}(y)=\beta} (e_x(f^{\circ D} - \alpha), e_y(g^{\circ D} - \beta))$$

where $e_Q(\phi)$ is the multiplicity of ϕ at Q . Combining the above with (3.1) and (3.2) we have

$$\begin{aligned} & h_{\text{gcd},S}(f^{\circ n}(a), g^{\circ n}(b)) \\ &= h_{\text{gcd},S}(f^{\circ D}(f^{\circ(n-D)}(a)), g^{\circ D}(g^{\circ(n-D)}(b))) \\ &\leq h_{\text{gcd},S}(F_1(f^{\circ(n-D)}(a)), G_1(g^{\circ(n-D)}(b))) \\ &\leq h_{\text{gcd},S}\left((F_1^{\text{red}} \circ f^{\circ(n-D)}(a))^{M'}, (G_1^{\text{red}} \circ g^{\circ(n-D)}(b))^{M'}\right) + O(1) \\ &\leq M' \cdot (4 \cdot h(f^{\circ(n-D)}(a)) + 4 \cdot h(g^{\circ(n-D)}(b)) + O(1)) + O(1) \text{ (by (3.2))} \\ &\leq M' \cdot (4d^{n-D} \cdot \hat{h}_f(a) + 4d^{n-D} \cdot \hat{h}_g(b) + O(1)) + O(1) \\ &\leq d^n \cdot \frac{M'}{d^D} \cdot (4\hat{h}_f(a) + 4\hat{h}_g(b) + C) + O(1). \end{aligned}$$

Since α, β are not exceptional for f, g respectively, by the proof of Lemma 3.52 of [19], we can choose $D = D(\varepsilon, f, g, a, b) \in \mathbb{N}$ sufficiently large so that

$$\frac{M'}{d^D} \cdot (4\hat{h}_f(a) + 4\hat{h}_g(b) + C) < \frac{\varepsilon}{2}.$$

Thus, we have

$$h_{\text{gcd},S}(f^{\circ n}(a), g^{\circ n}(b)) \leq \frac{\varepsilon}{2} \cdot d^n + O(1).$$

Hence in old coordinate we have

$$h_{\text{gcd},S}(f^{\circ n}(a) - \alpha, g^{\circ n}(b) - \beta) \leq \frac{\varepsilon}{2} \cdot d^n + O(1). \quad (3.3)$$

For any other (finite or infinite) place v , we use the old coordinate and we have

$$\begin{aligned} & \min(v^+(f^{\circ n}(a) - \alpha), v^+(g^{\circ n}(b) - \beta)) \\ &= \min\left(\max(-\log|f^{\circ n}(a) - \alpha|_v, 0), \max(-\log|g^{\circ n}(b) - \beta|_v, 0)\right). \end{aligned} \quad (3.4)$$

Since 0 is not exceptional with respect to f and to g , by Theorem E of [16], we know for all sufficiently large $n \in \mathbb{N}$,

$$\begin{aligned} -\log|f^{\circ n}(a) - \alpha|_v &\leq \frac{\varepsilon}{2 \cdot ([K : \mathbb{Q}] + |S|)} \cdot d^n + O(1), \\ -\log|g^{\circ n}(b) - \beta|_v &\leq \frac{\varepsilon}{2 \cdot ([K : \mathbb{Q}] + |S|)} \cdot d^n + O(1). \end{aligned} \quad (3.5)$$

Combining equations (3.3), (3.4) and (3.5), we obtain the requested estimate. \square

4 On the genericity condition

The Dynamical Mordell-Lang Conjecture predicts that given an endomorphism $\phi : X \rightarrow X$ of a complex quasi-projective variety X , for any point $P \in X$ and any sub-variety $Y \subsetneq X$, the set $\{n \in \mathbb{N} \mid \phi^{\circ n}(P) \in Y\}$ is a finite union of arithmetic progressions (sets of the form $\{a, a + d, a + 2d, \dots\}$ with $a, d \in \mathbb{N}_{\geq 0}$). The Dynamical Mordell-Lang Conjecture was proposed in [10]. See also [3] and [9] for earlier works. In the case of étale maps we know that the Dynamical Mordell-Lang Conjecture is true. See the recent monograph [4]. Xie proved in [21] the Dynamical Mordell-Lang Conjecture for polynomial endomorphisms of the affine plane.

Proof of Theorem 2.4. The result is clearly true in the case when (a, b) is preperiodic under (f, f) . When (a, b) is not preperiodic under (f, f) , by Theorem A it suffices to show that the sequence $(f^{\circ n}(a), f^{\circ n}(b))_n$ is generic. If there were infinitely many iterates $(f^{\circ n}(a), f^{\circ n}(b))$ lying on a curve C , by Theorem 0.1 of [21] the Dynamical Mordell-Lang Conjecture is true for polynomial endomorphisms of the affine plane. Therefore C itself is periodic under (f, f) . Replacing f by an iterate $f^{\circ m}$ we may assume that C is fixed under (f, f) . Now we can apply the results of [13] and [12] classification for invariant curves. In fact, using these results Baker and DeMarco demonstrated in Page 32 of [2] that the irreducible invariant curve in the above theorem must be a graph of the form $y = h(x)$ or $x = h(y)$, for a polynomial h which commutes with some $f^{\circ k}$ with initial conditions as in Theorem 2.4. This contradicts the assumption of Theorem 2.4. \square

We give two examples to show that if the assumption of Theorem 2.4 is not verified, then we might not have the upper bound.

Example 4.1. *Under the hypothesis of the above proof and use the same notations. Assume that the curve is given by $y = h(x)$ and $h \circ f^{\circ k} = f^{\circ k} \circ h$ for some $k \in \mathbb{N}_{>0}$. Suppose $n = mk$ with $k \in \mathbb{N}$. If $h(\alpha) = \alpha$, then*

$$\begin{aligned} \gcd(f^{\circ n}(a) - \alpha, f^{\circ n}(b) - \alpha) &= \gcd(f^{\circ mk}(a) - \alpha, f^{\circ mk}(h(a)) - \alpha) \\ &= \gcd(f^{\circ mk}(a) - \alpha, h(f^{\circ mk}(a)) - h(\alpha)) \\ &= |f^{\circ mk}(a) - \alpha| = |f^{\circ n}(a) - \alpha|. \end{aligned}$$

Example 4.2. *Let $f(x) = g(x) = x^3 + x$. Assume $a = -b$ and $\alpha = -\beta$. Then for $h(x) = -x$, we have $h \circ f = f \circ h$, $h(a) = b$ and $h(\alpha) = \beta$. Now*

$$f^{\circ n}(a) - \alpha = f^{\circ n}(-b) + \beta = -f^{\circ n}(b) + \beta = -(g^{\circ n}(b) - \beta),$$

so

$$\gcd(f^{\circ n}(a) - \alpha, g^{\circ n}(b) - \beta) = |f^{\circ n}(a) - \alpha| \gg |a|^{\delta^n}$$

for any $\delta < 3$.

In the case of power maps, if $(f^{\circ n}(a), g^{\circ n}(b))_n$ is generic, the following unconditional result is proved by Corvaja and Zannier ([6]).

Example 4.3. Suppose K is a number field and suppose $a, b, \alpha, \beta \in K$. Also suppose that f and g are power maps, and a, b are multiplicatively independent. Let $d = \max(\deg f, \deg g)$, then for each fixed $\varepsilon > 0$, there exists some $C = C(f, g, a, b)$ such that

$$\gcd(f^{\circ n}(a) - \alpha, g^{\circ n}(b) - \beta) \leq C \cdot \max(h(a), h(b))^{\varepsilon d^n}. \quad (4.1)$$

In fact, the genericity of the sequence $(f^{\circ n}(a), g^{\circ n}(b))_n$ is equivalent to the multiplicative independence of a and b . The assumption that α and β are not exceptional implies that $\alpha \neq 0$ and $\beta \neq 0$. Then Inequality (4.1) is a consequence of Inequality (1.2) of Corvaja and Zannier ([6]).

Now we provide an example to explain that the genericity of $(f^{\circ n}(a), f^{\circ n}(b))_n$ is necessary for power maps.

Example 4.4. Let $a = 125, b = 25, \alpha = \beta = 1, f(x) = x^2, g(y) = y^2$. Then $\gcd(f^{\circ n}(a) - \alpha, g^{\circ n}(b) - \beta)$ is divisible by $5^{2^n} - 1 = O((f^{\circ n}(a))^{1/3})$.

Acknowledgement

I want to express my gratitude to my advisor Thomas Tucker for suggesting this project and for valuable discussions, and to Wayne Peng for proofreading of this paper.

References

- [1] Nir Ailon and Zéev Rudnick. Torsion points on curves and common divisors of $a^k - 1$ and $b^k - 1$. *Acta Arith.*, 113(1):31–38, 2004.
- [2] Matthew Baker and Laura DeMarco. Special curves and postcritically finite polynomials. *Forum Math. Pi*, 1:e3, 35, 2013.
- [3] Jason P. Bell. A generalised Skolem-Mahler-Lech theorem for affine varieties. *J. London Math. Soc. (2)*, 73(2):367–379, 2006.
- [4] Jason P. Bell, Dragos Ghioca, and Thomas J. Tucker. *The Dynamical Mordell-Lang Conjecture*, volume 210. American Mathematical Soc., 2016.
- [5] Yann Bugeaud, Pietro Corvaja, and Umberto Zannier. An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$. *Math. Z.*, 243(1):79–84, 2003.
- [6] Pietro Corvaja and Umberto Zannier. A lower bound for the height of a rational function at S -unit points. *Monatsh. Math.*, 144(3):203–224, 2005.
- [7] Pietro Corvaja and Umberto Zannier. Some cases of Vojta’s conjecture on integral points over function fields. *J. Algebraic Geom.*, 17(2):295–333, 2008.
- [8] Pietro Corvaja and Umberto Zannier. Greatest common divisors of $u - 1, v - 1$ in positive characteristic and rational points on curves over finite fields. *J. Eur. Math. Soc. (JEMS)*, 15(5):1927–1942, 2013.

- [9] L. Denis. Géométrie diophantienne sur les modules de Drinfel'd. In *The arithmetic of function fields (Columbus, OH, 1991)*, volume 2 of *Ohio State Univ. Math. Res. Inst. Publ.*, pages 285–302. de Gruyter, Berlin, 1992.
- [10] D. Ghioca and T. J. Tucker. Periodic points, linearizing maps, and the dynamical Mordell-Lang problem. *J. Number Theory*, 129(6):1392–1403, 2009.
- [11] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.
- [12] Alice Medvedev and Thomas Scanlon. Invariant varieties for polynomial dynamical systems. *Ann. of Math. (2)*, 179(1):81–177, 2014.
- [13] Fedor Pakovich. Polynomial semiconjugacies, decompositions of iterations, and invariant curves. *Available at arXiv:1505.06351*, 2015.
- [14] Hector Pasten and Julie Tzu-Yueh Wang. GCD bounds for analytic functions. *International Mathematics Research Notices*, page rnw028, 2016.
- [15] Joseph H. Silverman. Arithmetic distance functions and height functions in Diophantine geometry. *Math. Ann.*, 279(2):193–216, 1987.
- [16] Joseph H. Silverman. Integer points, Diophantine approximation, and iteration of rational maps. *Duke Math. J.*, 71(3):793–829, 1993.
- [17] Joseph H. Silverman. Common divisors of $a^n - 1$ and $b^n - 1$ over function fields. *New York J. Math.*, 10:37–43 (electronic), 2004.
- [18] Joseph H. Silverman. Generalized greatest common divisors, divisibility sequences, and Vojta's conjecture for blowups. *Monatsh. Math.*, 145(4):333–350, 2005.
- [19] Joseph H. Silverman. *The arithmetic of dynamical systems*, volume 241 of *Graduate Texts in Mathematics*. Springer, New York, 2007.
- [20] Paul Vojta. *Diophantine approximations and value distribution theory*, volume 1239 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1987.
- [21] Junyi Xie. The Dynamical Mordell-Lang Conjecture for polynomial endomorphisms of the affine plane. *Available at arXiv:1503.00773*, 2015.